AARC Authentication and Authorisation for Research and Collaboration

Can we trust eduGAIN?

Authentication and Authorisation for Research and Collaboration

Hannah Short
AARC
Computer Security, CERN

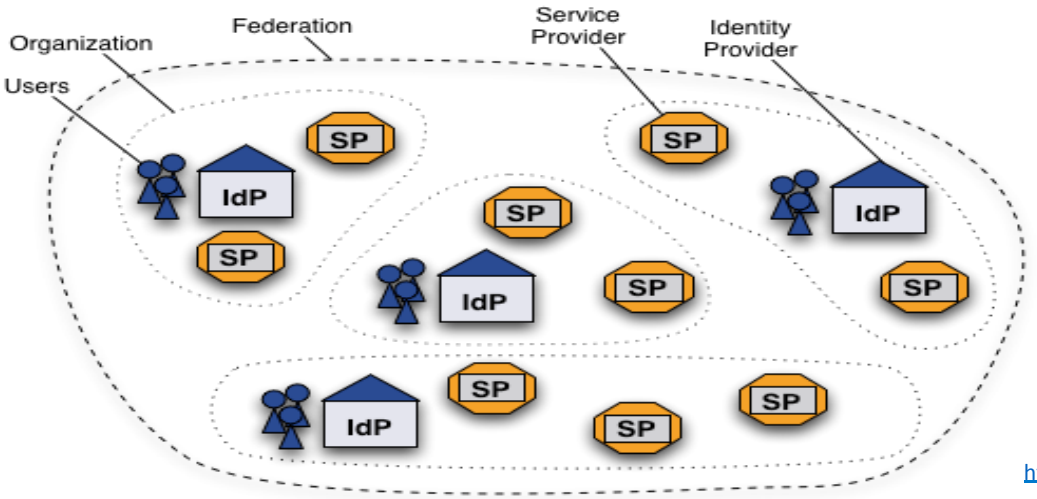
HEPiX
18 October 2016

What will we talk about?

- What is eduGAIN?
- What is trust?
- What concerns do we have over eduGAIN?
- Security Incident Response

Federated Identity Management Worldwide
What is a Federation?

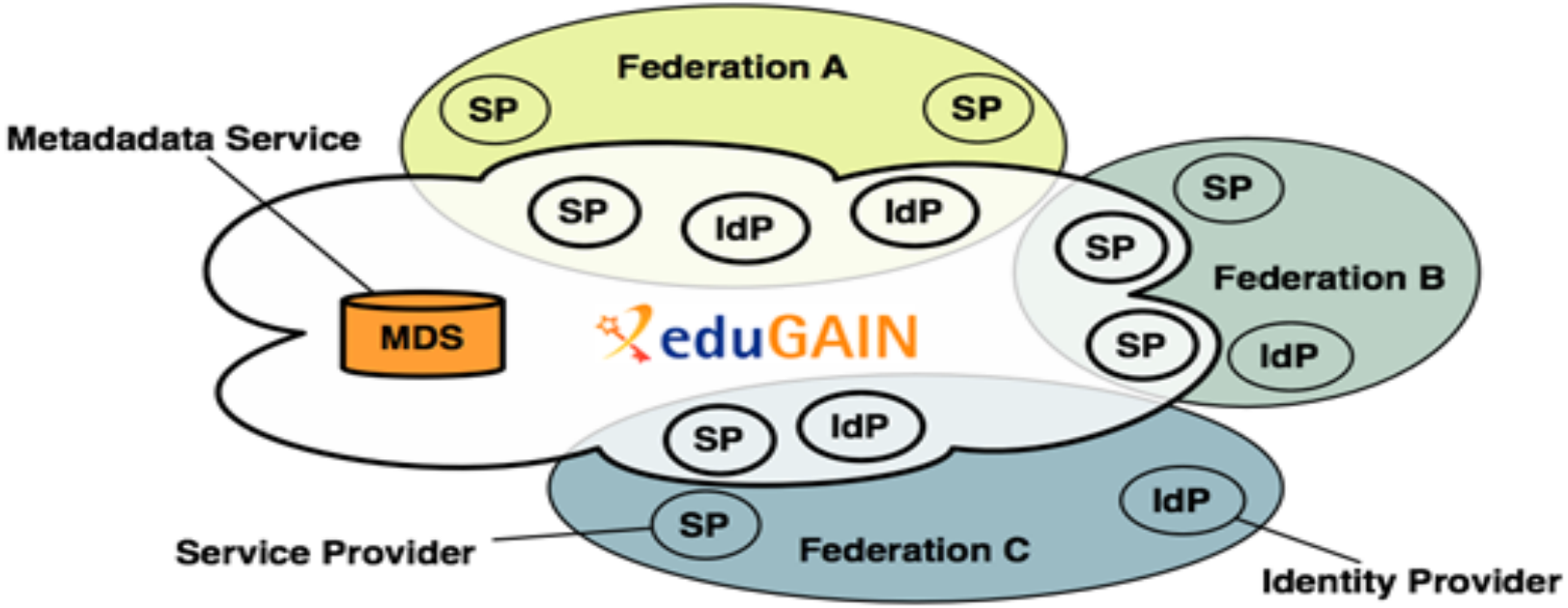
- Federated Identity Mangement (FIM) is the concept of groups of Service Providers (SPs) and Identity Providers (IdPs) agreeing to interoperate under a set of policies.
- Federations are typically established nationally and use the SAML2 protocol for information exchange
- Each entity within the federation is described by metadata



https://www.switch.ch/aai/about/federation/

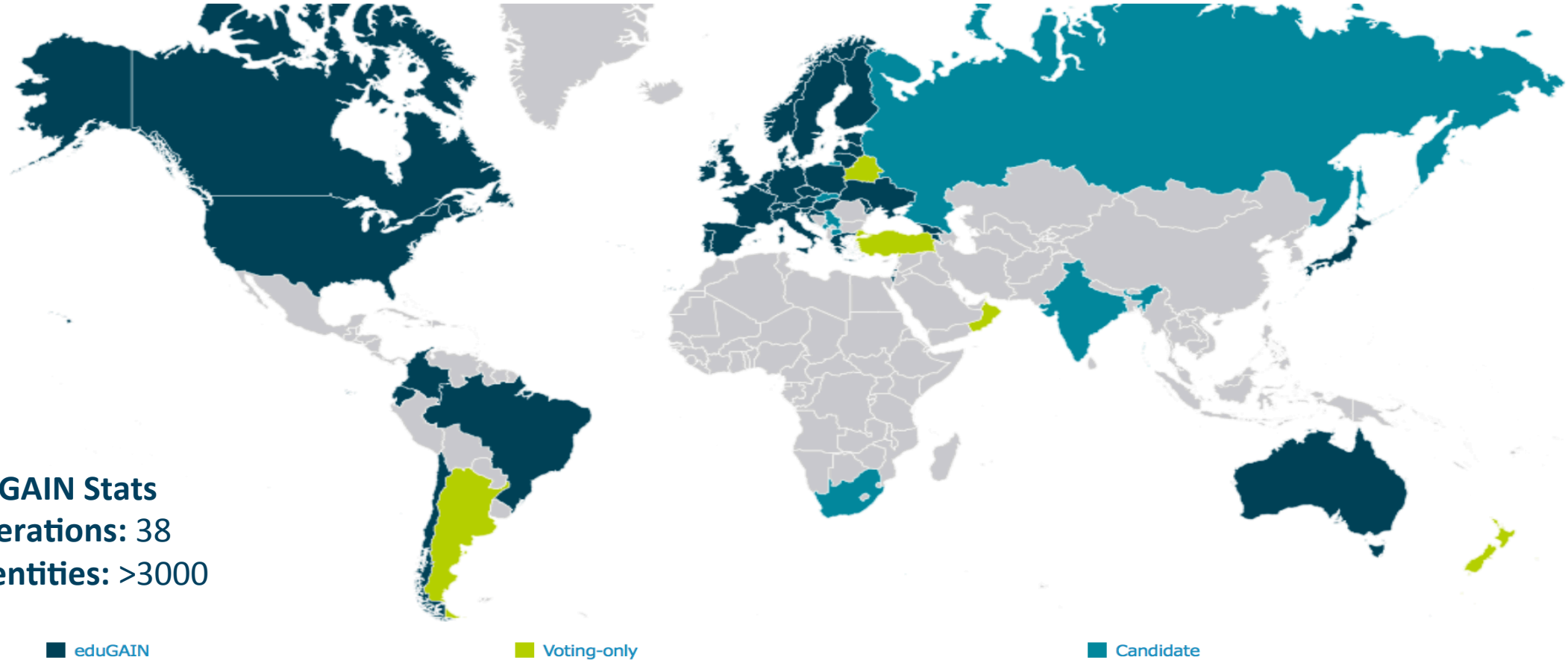
Federated Identity Management Worldwide
eduGAIN

- eduGAIN is a form of interfederation
- Participating federations share information (metadata) about entities from their own federation with eduGAIN
- eduGAIN bundles this metadata and publishes it in a central location.



Credit to Alessandra Scicchitano – GEANT for this slide

Federated Identity Management Worldwide
eduGAIN adoption



eduGAIN Stats
Federations: 38
All entities: >3000

Credit to eduGAIN, data taken March 2016

2037 IdPs

Potential sources of compromised identities

1197 SPs

Potential targets

What is trust?

Typically refer to vectors of trust relating to the identity such as:

Identity Proofing

- how strongly the set of identity attributes have been verified and vetted

Credential Binding

- how likely it is that the right person is presenting the credential to the identity provider

Assertion Presentation

- how well the given digital identity can be communicated across the network without information leaking to unintended parties, and without spoofing

https://tools.ietf.org/html/draft-richer-vectors-of-trust-00#section-3.1

What is trust?

- But trust is more than confidence in the identity
- We need to trust that the organisation will be able and willing to collaborate in effective security incident response!

Identity Proofing

- how strongly the set of identity attributes have been verified and vetted

Credential Binding

- how likely it is that the right person is presenting the credential to the identity provider

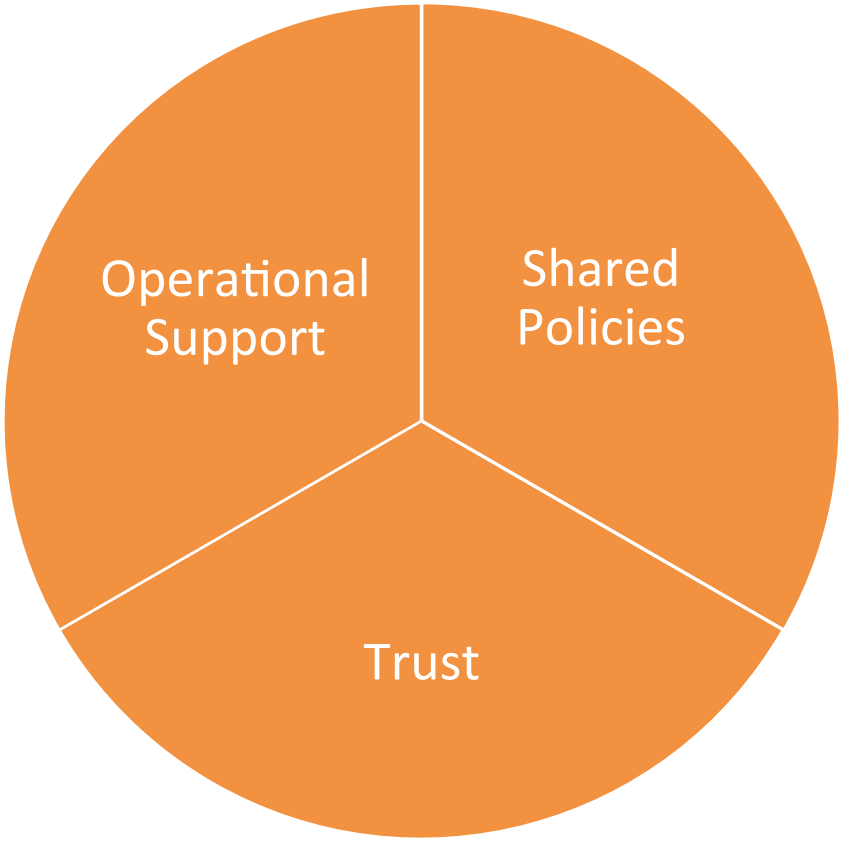
Assertion Presentation

- how well the given digital identity can be communicated across the network without information leaking to unintended parties, and without spoofing

Security Capability

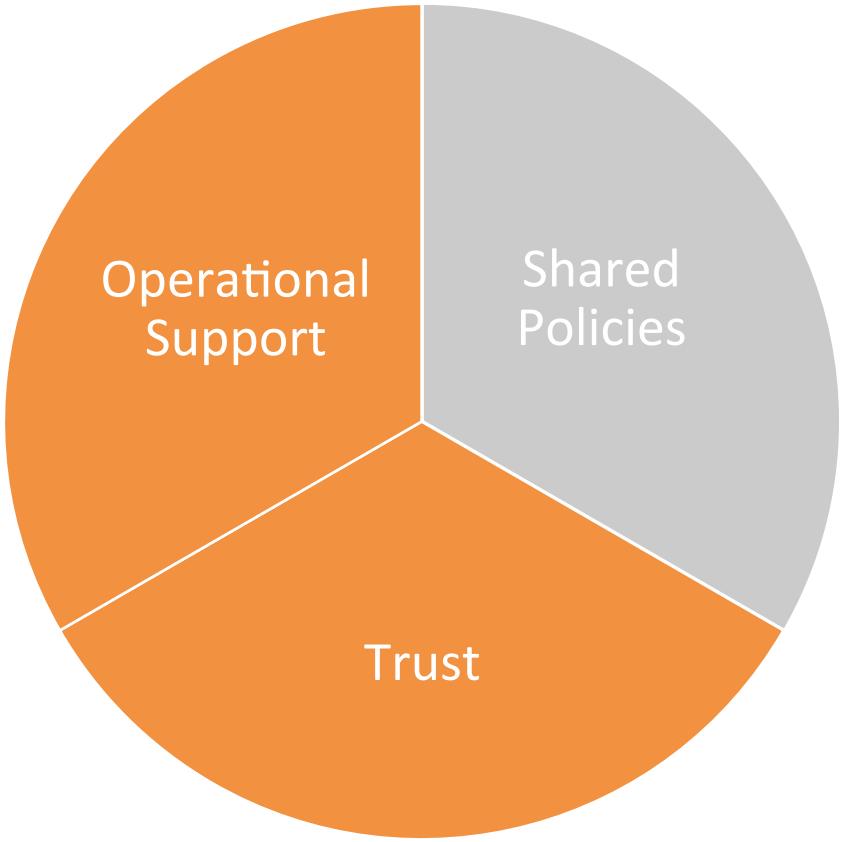
- how effectively will an organisation participate in Security Incident Response

What is required for effective Security Incident Response?



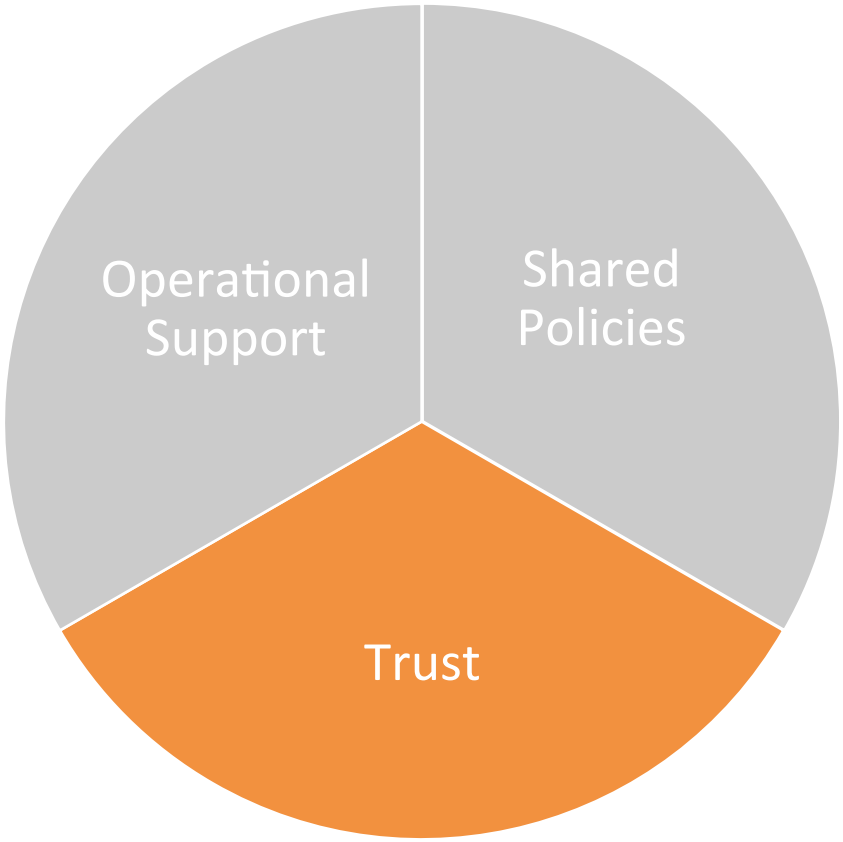
The challenge of Federated Identity Management

- EduGAIN membership includes 4 policies… Security Incident Response is not one
- We have no insight into security practices of each participant
- Collaboration between IdPs and SPs is essential to build full incident timeline – they have no obligation to collaborate



The challenge of Federated Identity Management

- EduGAIN has no central help desk
- Few national federations offer central security support
- No way to block an identity, IdP, or federation <u>everywhere</u> and <u>immediately</u>

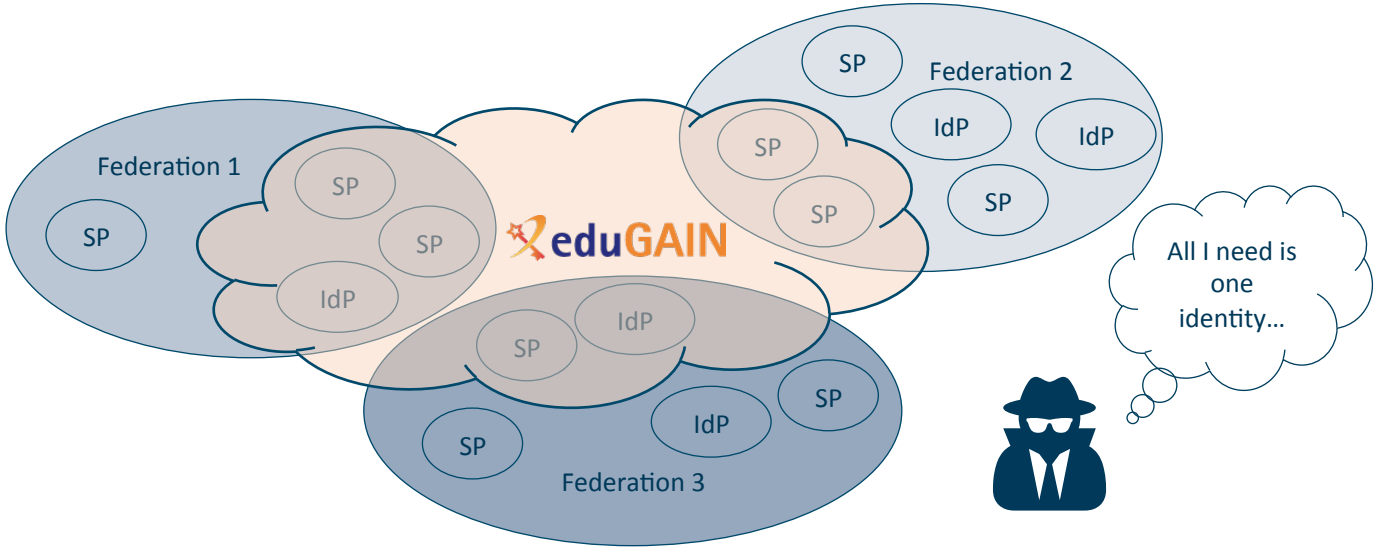


The challenge of Federated Identity Management

- Security is often not priority (or even in skillset) of engaged FIM participants

- Simply too big…

What can we do?



Clearly an inviting vector of attack… luckily, this was noticed several years ago!

Beginnings

- Issues of IdM raised by IT leaders from EIROforum labs (Jan 2011)
  - CERN, EFDA-JET, EMBL, ESA, ESO, ESRF, European XFEL and ILL
  - These laboratories, as well as national and regional research organizations, face similar challenges

- Prepared a paper that documents common requirements
  https://cdsweb.cern.ch/record/1442597

"Security procedures and incident response would need to be reviewed. Today, each resource provider is for example responsible for terminating access by known compromised identities. With identity federation, this responsibility will be shifted to the IdP though resource providers will insist on the ability to revoke access."

"Such an identity federation in the High Energy Physics (HEP) community would rely on:
*• A well-defined **framework** to ensure sufficient **trust** and **security** among the different IdPs and relying parties."*

Credit to David Kelsey (STFC) for this content

Evolution

Several years later, 2016

Security
Incident
Response
Trust Framework for
Federated
Identity

✓Approved by the REFEDS (Research & Education FEDerations) Community

✓Registered Internet Assigned Numbers Authority (IANA) Assurance Profile
https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml

Sirtfi

Operational Security

- Require that a security incident response capability exists with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration

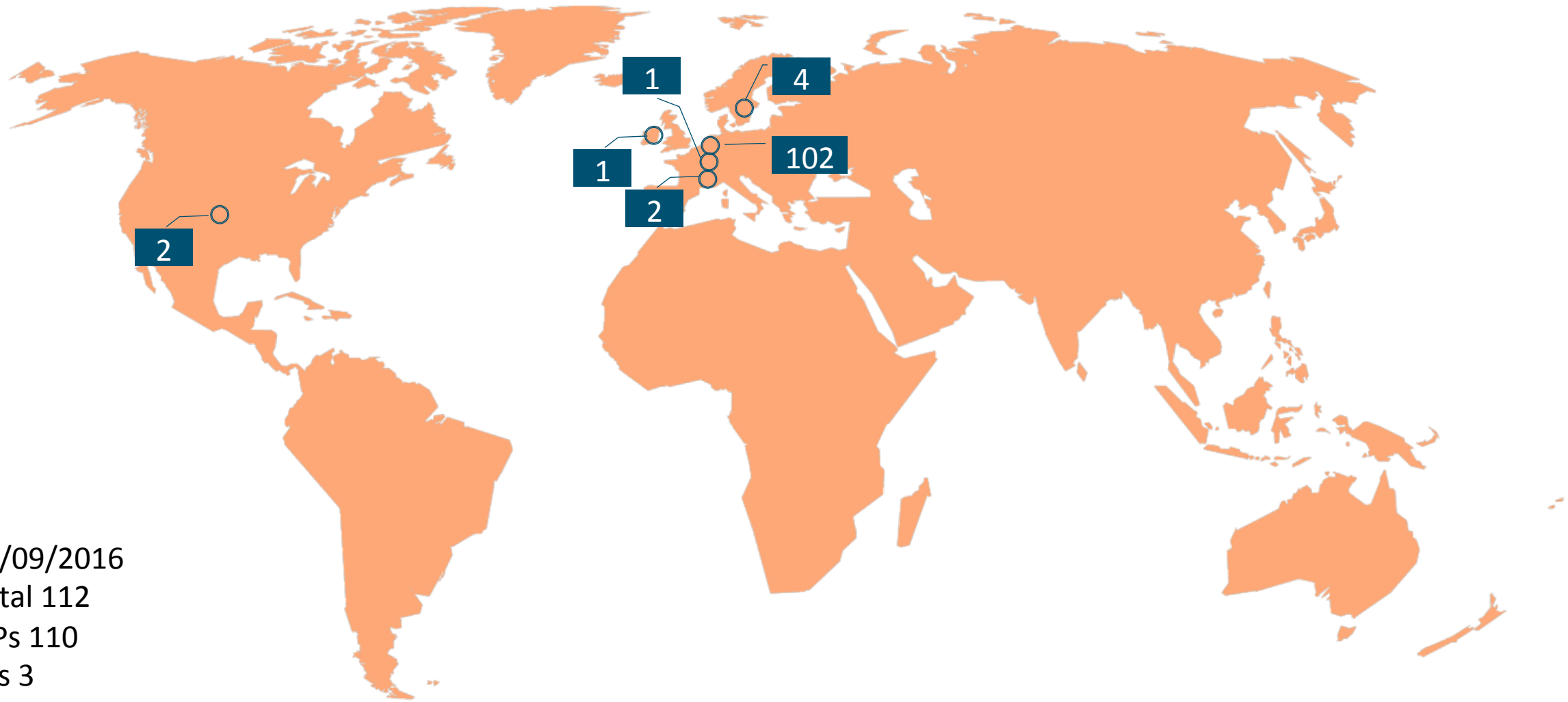
Traceability

- Improve the usefulness of logs
- Ensure logs are kept in accordance with policy

Participant Responsibilities

- Confirm that end users are aware of an appropriate AUP

Current adoption



22/09/2016
Total 112
IdPs 110
SPs 3

Find out more

Call us : +31(0)20 5304488 Mail us : contact@refeds.org

REFEDS

Home Blog Wiki Meetings Sponsor Federations Our Work About

SIRTFI **https://refeds.org/sirtfi** REFEDS > SIRTFI

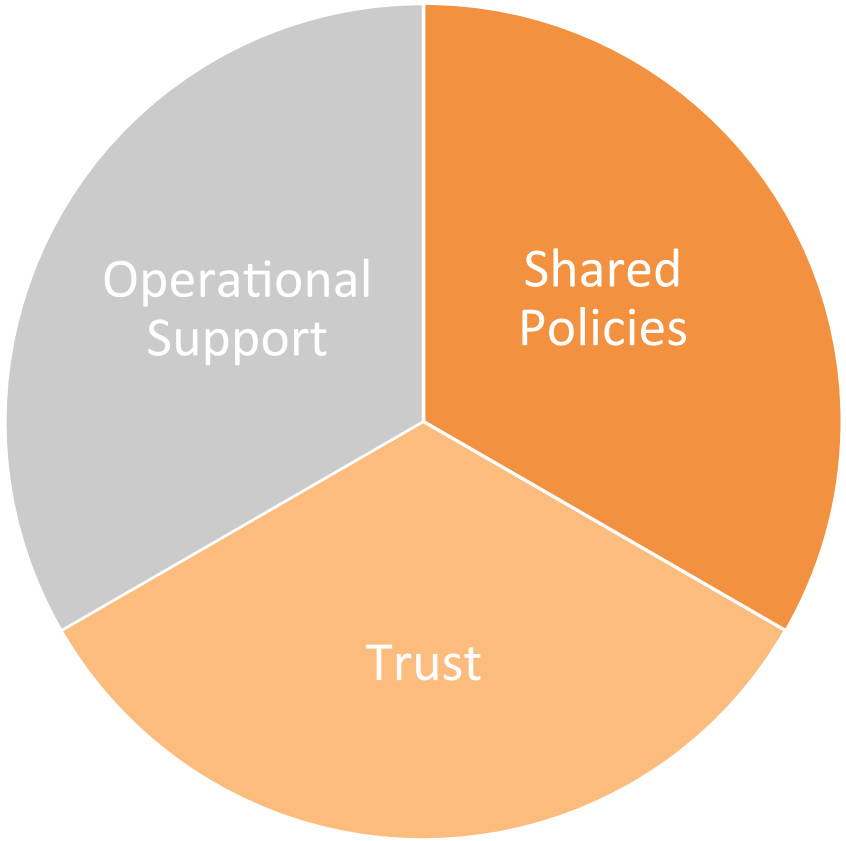
The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant.

REFEDS' Sirtfi Working Group has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC Project.

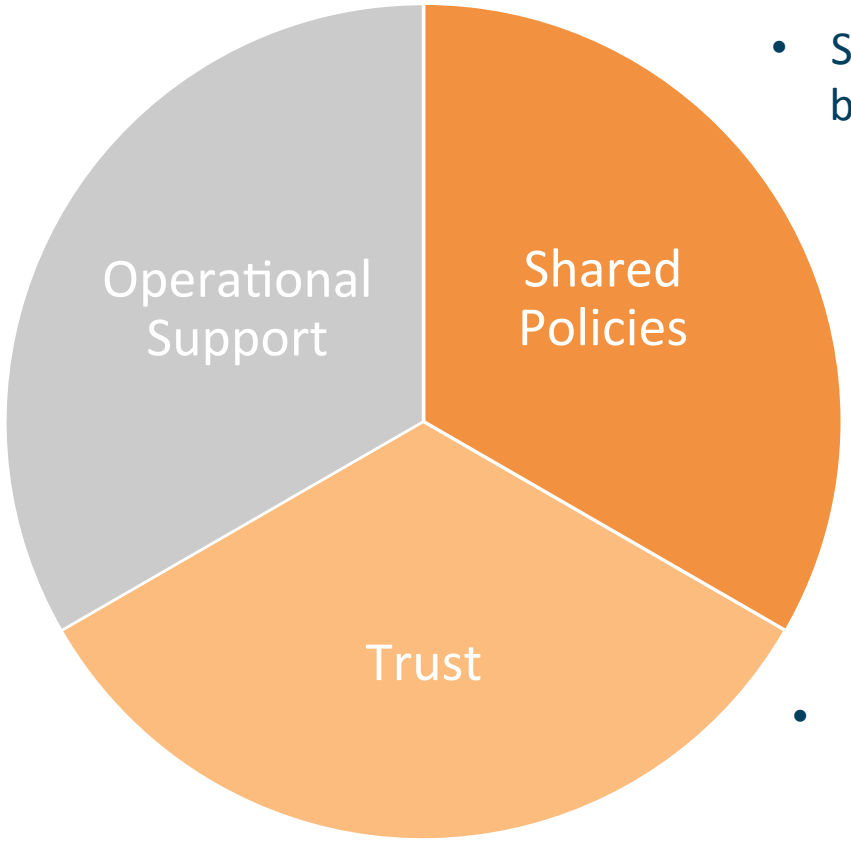
Benefits	Sirtfi v 1.0	FAQs
Why should I join? What are the Benefits?	View the Sirtfi Framework	Need help?

How does Sirtfi help?

How does Sirtfi help?



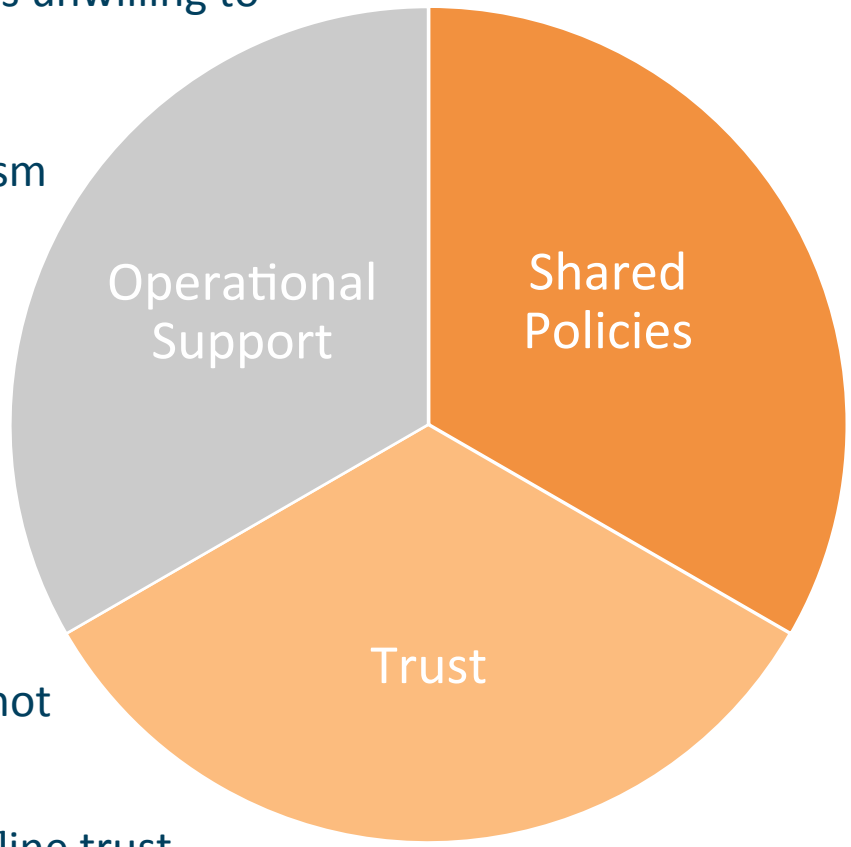
How does Sirtfi help?



- Shared framework fulfills purpose of basic policy
  - Obliged to collaborate
    - Basic operational security best practices
- Allows us to identify security conscious bodies

How does Sirtfi not help?

- Some Federation Operators unwilling to act as gatekeepers
- No large-scale blocking mechanism

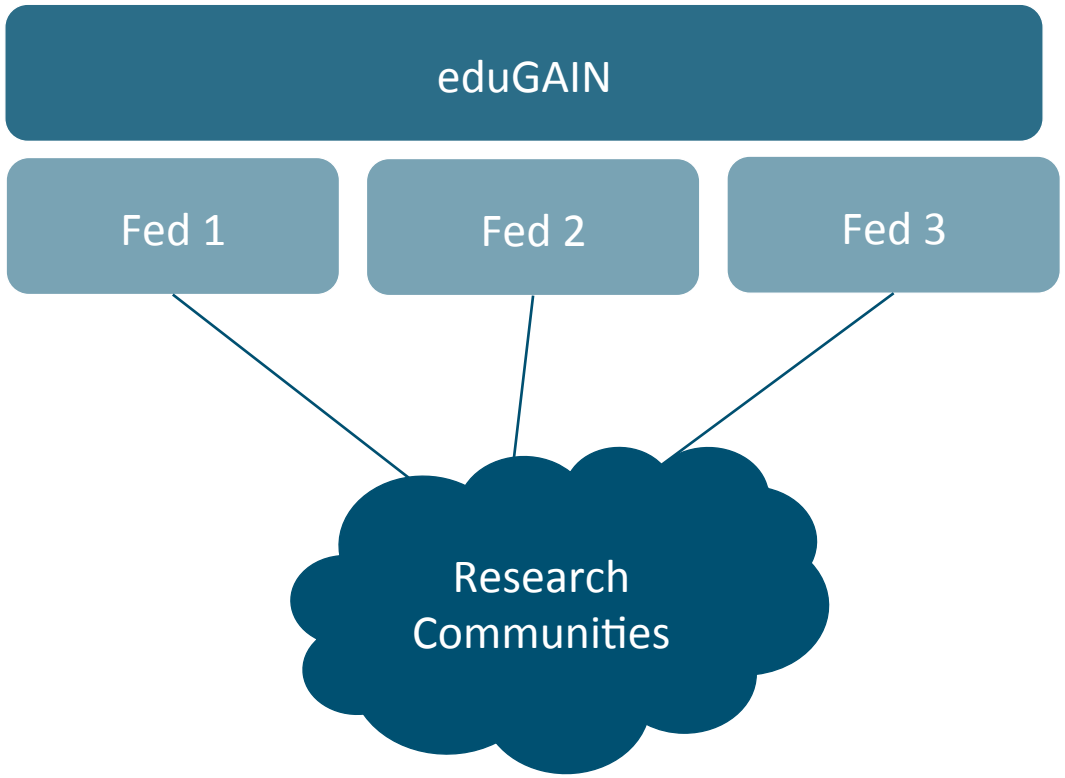


- Trust tied to organisation/entity, not individual
  - Difficult to build offline trust

What's missing?

Requirement	How could we get this?
Indication of who really trusts who	Independent trust portal, votes based web of trust
Capability to remove participants from Sirtfi	Shared Operational Support
Periodic tests of contact responsiveness	
Channel for smaller participants to access security support and trust groups	
Log of "bad behaviour"	
Ability to block identities across eduGAIN	Distributed mechanism for blocking users (e.g. confyrm, perun…)

Operational Support is needed, but where?

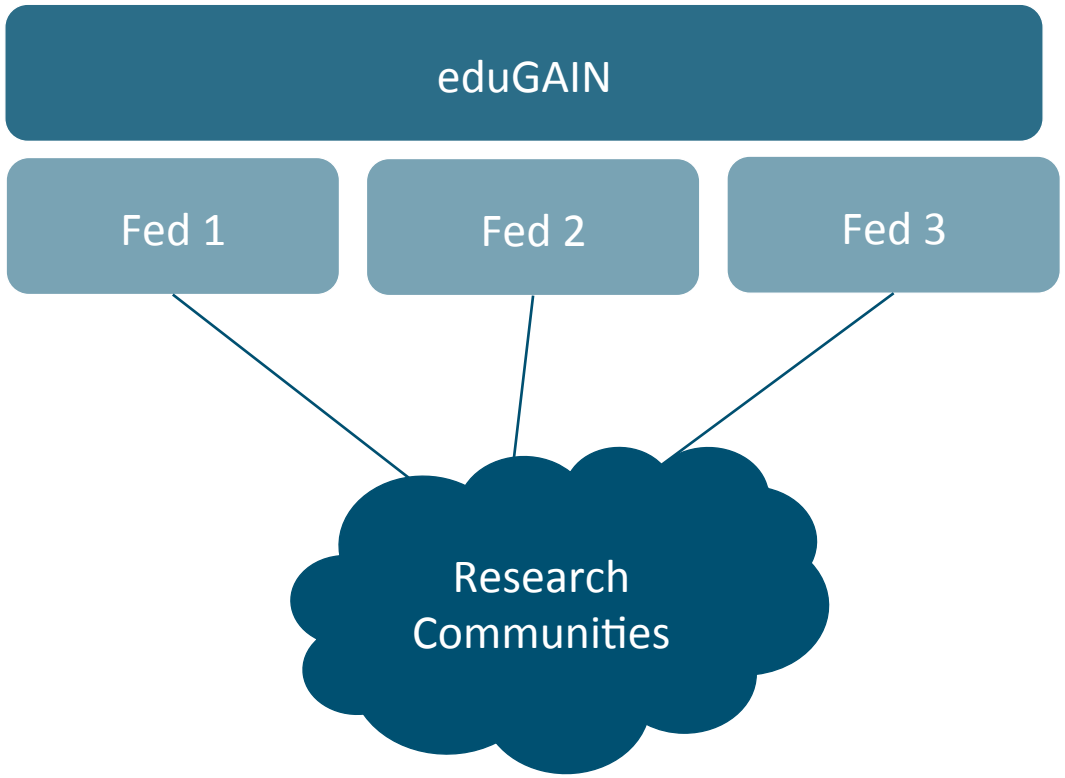


eduGAIN – no central support

Federations – not all are willing

Research Communities – very possible!

Operational Support is needed, but where?

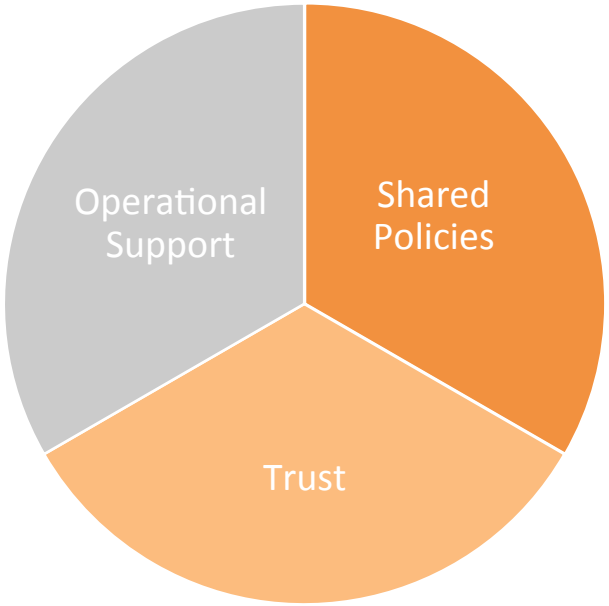


The Interoperable Global Trust Federation (IGTF) is interested in supporting this work.

Objective to ensure that authentication with an eduGAIN identity is as secure as with an x.509 certificate.

Conclusion

- Trust is hard to build and easy to break
- Trust is not inherently present in eduGAIN
- There is a need to establish an effective Security Incident Response capability within eduGAIN
- Sirtfi goes some way to providing the missing capabilities
- There are still gaps, particularly for sustainable operational support



Thank you

Any Questions?

hannah.short@cern.ch

https://aarc-project.eu

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).